REMARKS

I. Introduction

In response to the Office Action dated October 3, 2005, claims 1, 6, 10, 15, 19, 24, 28, and 33 have been amended. Claims 1-36 remain in the application. Re-examination and re-consideration of the application, as amended, is requested.

II. Non-Art Rejections

On page (2) of the Office Action, claims 6, 15, 24, and 33 were rejected under 35 U.S.C. §112, second paragraph, as being indefinite because in claims 6, 15, 24, and 33 they recite the limitation from the microprocessor and there is insufficient antecedent basis for this limitation in the claim. Applicants have amended claims 6, 15, 24, and 33 to overcome this rejection and submit that the rejection is now moot.

III. Prior Art Rejections

In paragraphs (1)-(6) of the Office Action, claims 19, 20, 22, 23, and 26 were rejected under 35 U.S.C. §102(e) as being anticipated by Kocher, U.S. Patent No. 6,289,455. In paragraphs (7)-(12) of the Office Action, claims 1, 2, 4, 5, and 8 were rejected under 35 U.S.C. §103(a) as being unpatentable over Cohen, U.S. Patent No. 5,282,249, in view of Kocher. In paragraphs (13)-(17) of the Office Action, claims 3, 6, and 7 were rejected under 35 U.S.C. §103(a) as being unpatentable over Cohen, in view of Kocher, and further in view of Pitts, U.S. Publication No. 2002/0145931. In paragraphs (18)-(31) of the Office Action, claims 10, 11, 13, 14, 17, 18, 27-29, 31, 32, 35, and 36 were rejected under 35 U.S.C. §103(a) as being unpatentable over Kocher, in view of Barth, U.S. Patent No. 6,334,216. In paragraphs (32)-(42) of the Office Action, claims 12, 15, 16, 30, 33, and 34 were rejected under 35 U.S.C. §103(a) as being unpatentable over Kocher, in view of Barth, and further in view of Pitts.

Specifically, independent claims 1, 10, 19, and 28 were rejected as follows:

> As to claim 19, Kocher discloses a conditional access module (CAM), (Fig. 2 #225 wherein the CAM is the cryptographic rights unit) comprising:
> a nonvolatile memory component (column 21, lines 13-15), wherein:
> the nonvolatile memory component is used to contain state information to provide desired functionality and enforce one or more security policies for accessing the digital services (column 10, lines 36-38 and 43-47 wherein the digital services is pay-tv); and
> the nonvolatile memory component is protected from modification such that the nonvolatile memory component is read only (column 10, lines 43-47); and

access to the nonvolatile memory component is isolated (Fig. 2 #265);

a hidden non-modifiable identification number embedded into the nonvolatile memory component, wherein the identification number uniquely identifies the CAM (column 18 lines 37-45 wherein the identification number is the serial number alluded to and which is stored in the protected memory and is non-modifiable in the same manner as the unique BATCH_KEY described in column 18, lines 49-52); and

a fixed state custom logic block, wherein the nonvolatile memory component is not directly accessible via a system bus and access to the nonvolatile memory component is not directly accessible via a system bus and access to the nonvolatile memory component is limited to the custom logic block (Fig. 2 #260 wherein the CryptoFirewall is the custom logic block).

As to claim 1, Cohen discloses a system for controlling access to digital services comprising:

(a) A control center configured to coordinate and provide digital services (see Fig. 2);

(b) An uplink center configured to receive the digital services from the control center and transmit the digital services to a satellite (see Fig. 1/1 #20);

(c) The satellite configured to:

Receive the digital services from the uplink center (Fig. 1/2 #22);

Process the digital services (Fig. 1/2 #22 wherein processing of digital services is the intrinsic step that allows transmission); and

Transmit the digital services to a subscriber receiver station (Fig. 1/2 #24);

(d) The subscriber receiver station configured to:

Receive the digital services from the satellite (Fig.1/2 #26);

Control access to the digital services through an integrated receiver/decoder (IRD) (Fig. 1/2 #30);

(e) A conditional access module (CAM) communicatively coupled to the IRD (Fig. 1/2 #32);

but does not disclose wherein the CAM comprises:

a nonvolatile memory component, wherein:

the nonvolatile memory component is used to contain state information to provide desired functionality and enforce one or more security policies for accessing the digital services; and

the nonvolatile memory component is used to contain state information to provide desired functionality and enforce one or more security policies for accessing the digital services; and

the nonvolatile memory component is protected from modification such that the nonvolatile memory component is isolated;

a hidden non-modifiable identification number embedded into the nonvolatile memory component, wherein the identification number uniquely identifies the CAM; and

a fixed state custom logic block, wherein the nonvolatile memory component is not directly accessible via a system bus and access to the nonvolatile memory component is limited to the custom logic block.

Kocher discloses wherein the CAM (Fig. 2 #225 wherein the CAM is the cryptographic rights unit) comprises:

a nonvolatile memory component (column 21, lines 13-15), wherein:

the nonvolatile memory component is used to contain state information to provide desired functionality and enforce one or more security policies for accessing the digital services (column 10, lines 36-38 and 43-47 wherein the digital services is pay-tv); and

the nonvolatile memory component is protected from modification such that the nonvolatile memory component is read only (column 10, lines 43-47); and

access to the nonvolatile memory component is isolated (Fig. 2 #265);

a hidden non-modifiable identification number embedded into the nonvolatile memory component, wherein the identification number uniquely identifies the CAM (column 18, lines 37-45 wherein the identification number is the serial number alluded to and which is stored in the protected memory and is non-modifiable in the same manner as the unique BATCH_KEY described in column 18, lines 49-52); and

a fixed state custom logic block, wherein the nonvolatile memory component is not directly accessible via a system bus and access to the nonvolatile memory component is limited to the custom logic block (Fig. 2 #260 wherein the CryptoFirewall is the custom logic block).

Kocher is analogous art because it discusses a method and apparatus for preventing piracy of digital content including the use of a smart card.

It would have been obvious at the time of the invention to include the features of the CAM found in Kocher in this smart card used by Cohen to control access to the broadcasted data.

Motivation for one to modify Cohen as discussed above would have been to improve the security of systems used to distribute and protect digital content (from piracy or attackers) as taught in Kocher (column 5, lines 55-56).

As to claim 10, Kocher discloses a method for limiting unauthorized access to digital services comprising:

Embedding a hidden non-modifiable identification number into a nonvolatile memory component (column 21, lines 13-15 and column 18, lines 37-45 wherein the identification number is the serial number alluded to and which is stored in the protected memory and is non-modifiable in the same manner as the unique BATCH_KEY described in column 18, lines 49-52), wherein:

The nonvolatile memory component is used to contain state information to provide desired functionality and enforce one or more security policies for accessing the digital services (column 10, lines 36-38 and 43-47 wherein the digital services is pay-tv);

The hidden non-modifiable identification number uniquely identifies a device containing the nonvolatile memory component (column 18, lines 37-45); and

Isolating access to the nonvolatile memory component such that access to the nonvolatile memory component is limited to a fixed state custom logic block (Fig. 2 #260 wherein the CryptoFirewall is the custom logic block as described in column 21, lines 34-35), the nonvolatile memory component is protected such that the nonvolatile memory component is read only (column 10, lines 43-47), and the nonvolatile memory component is not directly accessible via a system bus (Fig. 2 #260).

But does not disclose wherein access to the digital services is based on access rights associated with the hidden non-modifiable identification number.

Barth does disclose wherein access to the digital services is based on access rights associated with an identification number (column 4, lines 33-45 wherein the access rights is whether it is associated with a blocking note).

Barth is analogous art because it discloses a method a gaining access to services based on an identification number utilized in an access card.

It would have been obvious for one of ordinary skill in the art at the time of the invention to modify Kocher to include the method of comparing an identification number to a list of unauthorized numbers and their access rights before granting access.

Motivation for one to modify Kocher as discussed above would have been to allow system management to prevent access to the service if the corresponding number is reported as lost or if the user is delinquent in his obligations for the services offered as taught in Barth (column 3, lines 37-42).

As to claim 28, it is rejected because it discusses the same subject matter as claim 10.

Applicant traverses the above rejections for one or more of the following reasons:

(1) The cited references fail to teach, disclose or suggest the use of an identification number; and

(2) The cited references fail to teach, disclose or suggest the use of an identification number that is used to limit a cloning attack wherein said cloning attack comprises copying the identification number to a new CAM.

Independent claims 1, 10, 19, and 28 are generally directed to the use of an identification number. Specifically, the claims address an identification number that is used to limit a cloning attack. As set forth throughout the specification (including paragraphs [0062], [0072]-[0074], and [0078]), the identification number uniquely identifies the device (i.e., the CAM) and such an identifier is used in a particular context. In this regard, the amended claims specifically provide that the identification number is used to limit a cloning attack wherein such a cloning attack comprises copying the identification number to a new pirated CAM. As indicated in the specification, hacking techniques typically use a low cost cloning attack wherein the identity of a pirate card is copied to a new card. The claims provide for hiding this identification number in the isolated nonvolatile memory component. By preventing access to the identification number (except through the custom logic block), the low cost cloning attack techniques are limited.

The cited references do not teach nor suggest these various elements of Applicants' independent claims. In comparing the prior art, it is necessary to have a complete understanding of the prior art and its use of keys and identification numbers. As described above, identification numbers for a card are unique and are used in a particular context. Keys are also used in a particular context. In this regard, keys in the prior art (including the device keys and batch keys described in Kocher), are used to encrypt service keys (such as Kocher's rights keys) that are then used to derive control words (such as Kocher's content decryption keys) for decrypting content. However, the unique card identification number is not used to directly generate control words. In this regard, Kocher fails to describe the use of an identification number.

However, as known in the art, the identification number is used to determine which key to use, or to generate the key that is then used, or to address a key delivery message, or to identify devices that are permitted or excluded from access to services. In this regard, there is a significant difference between the use of keys and identification numbers in the field of art.

It is also worth noting that since the identification numbers are unique to a particular card and may be used to generate a device key, the key would also be unique to the card. In view of such a key generation, the keys are clearly different from an identification number. For example, a key

cannot be merely copied to new card and thereby clone the card. However, if the identification number is copied to a new card, a cloned card would be created. These facts clearly differentiate an identification number from a key.

Since the identification numbers are unique to a particular card and may be used to address a message for transmitting a key for generating control words, the delivery of said key may be limited to cards that subscribe to said service. In view of such a key delivery, the keys are clearly different from an identification number. However, if the identification number is copied to a new card, a cloned card would be created which would also receive the addressed key message. These facts clearly differentiate an identification number from a key.

In view of the differences between a key and identification number, it should be noted that Kocher does not address the use of an identification number whatsoever but merely describes the use of a key (see Abstract; col. 7, lines 65-67; col. 8, lines 52-55; col. 10, lines 36-47; etc.). In this regard, Kocher explicitly provides for storing the keys (and not the identification number) in protected memory. Such keys of Kocher are used during the decryption process to view data. Again, the keys are specifically used in the encryption/decryption of content and are not used like an identification number to select a key to use during the encryption/decryption process.

The claims as amended provide that the hidden identification number is used to limit a cloning attack wherein the identity of the card is transferred/copied to another card. Such a limitation clearly establishes a difference with a key that cannot be used in such a cloning attack but is used in another attacking/hacking context (e.g., during encryption/decryption). Accordingly, the use of such anti-cloning language in the claims in combination with a limitation that expressly provides that the identification number uniquely identifies the CAM/device; Applicants submit that Kocher does not and cannot teach, disclose, or suggest, explicitly or implicitly, the presently claimed invention.

Further, since the Kocher stores the keys in protected memory, there would be no need to store the identification number itself in protected memory. In this regard, Kocher would be required to have access to the identification number in order to select a particular key in the protected memory. Accordingly, Kocher actually teaches away from the storage of the identification number in protected memory (as claimed).

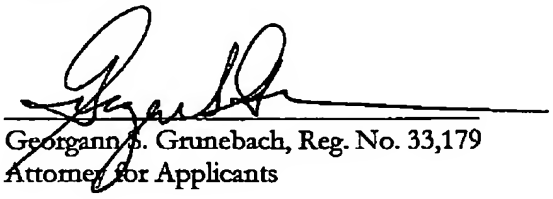
Moreover, the various elements of Applicants' claimed invention together provide operational advantages over Kocher, Cohen, and Pitts, Barth (e.g., with respect to preventing cloning attacks). In addition, Applicants' invention solves problems not recognized by Kocher, Cohen, and Pitts, Barth.

Thus, Applicants submit that independent claims 1, 10, 19, and 28 are allowable over Kocher, Cohen, and Pitts, Barth. Further, dependent claims 2-9, 11-18, 20-27, and 29-36 are submitted to be allowable over Kocher, Cohen, and Pitts, Barth in the same manner, because they are dependent on independent claims 1, 10, 19, and 28, respectively, and thus contain all the limitations of the independent claims. In addition, dependent claims 2-9, 11-18, 20-27, and 29-36 recite additional novel elements not shown by Kocher, Cohen, and Pitts, Barth.

IV. Conclusion

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited. Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.

Respectfully submitted,



Georgann S. Grunebach, Reg. No. 33,179
Attorney for Applicants

Date: February 3, 2006

The DIRECTV Group, Inc.
RE / R11 / A109
P.O. Box 1450
2250 E. Imperial Highway
El Segundo, CA 90245-0956

Phone: (310) 964-4615